New *Handbook for Chapter 13 Standing Trustees* Provides Updated Guidance

By Martha Hallowell, Deputy Assistant Director,
Standing Trustee Oversight, Office of Oversight, Executive Office for U.S. Trustees

Introduction

By this time, standing trustees and their staffs have had the opportunity to read and digest the new *Handbook for Chapter 13 Standing Trustees* (Handbook), which took effect on October 1, 2012. The updated Handbook incorporates many practices and policies developed since the Handbook was first issued in 1998, and it is substantially reorganized. This article focuses on four areas of particular interest – required questions at the section 341 meeting, employee vacancies, vendor fidelity coverage and background checks, and computer security.

For convenient reference, the Handbook is posted at http://www.justice.gov/ust/eo/private_trustee/library/chapter13/index.htm along with a Summary of Changes.

Required Questions at Section 341 Meeting

Responding to sensitivities about the potential release of personally identifiable information (PII), the U.S. Trustee Program (Program or USTP) modified the first required question at the section 341 meeting of creditors. Debtors no longer need to state on the record their current home address. Instead, standing trustees should ask debtors if the address on the petition is their current address.

The Program has adopted the definition of PII used by the Office of Management and Budget: "[i]nformation which can be used to distinguish or trace an individual's identity … alone, or when combined with other personal or identifying information." A debtor's name and address, when combined, meet this definition. This change protects the debtor's privacy and physical security.

Employee Vacancies

The Handbook imposes new requirements on a standing trustee who is faced with a staff vacancy. While the USTP does not wish to impose its business judgment in place of the trustee's in hiring matters, the trustee should solicit interest from a diverse pool of potential applicants. To that end, the USTP now requires that, when filling new positions or vacancies, the trustee place advertisements, conduct interviews and otherwise ensure an open hiring process.

This requirement does not apply when the trustee is filling the new position or vacancy internally. The USTP encourages promotion from within when a qualified candidate is on staff. In addition, the standing trustee need not advertise when filling a vacancy with a person who came to the standing trustee's employ through a temporary agency.

Vendor Fidelity Coverage and Background Checks

The standing trustee has a duty to be accountable for all property received in an estate. Standing trustees rely on case administration software to track funds received and funds distributed. As such, it is critical that access to that software and data is restricted to those with a need for such access, and that there is adequate separation of duties. The Handbook imposes two new requirements designed to protect the trustee and the data maintained by the trustee.

First, standing trustees must select software providers who maintain a reasonable amount of fidelity coverage on their own employees. Software vendors require significant access to the case administration software to ensure it is working properly. The trustee monitors the vendors' activities through various reports, but the fidelity coverage provides the trustee with an additional layer of protection in the event safeguards are circumvented and a vendor's employee misappropriates funds.

Second, the standing trustee must ensure that any consultants or vendors retained by the trustee who have the ability to change live data in the computer system have undergone criminal background checks, to the extent authorized by state law.

The Executive Office for U.S. Trustees solicited information regarding these two requirements from the software vendors and provided that information to leadership in the National Association of Chapter 13 Trustees and to Program personnel for dissemination to standing trustees.

Computer Security

As standing trustees and their staff more frequently access office computer files from remote locations such as courthouses or their homes, potential security vulnerabilities arise. Case data must be protected from loss or compromise. The USTP has expanded its computer security policies and the Handbook now includes a discussion of remote access. The Handbook recommends a virtual private network (VPN) solution to ensure the remote connection is secure. In addition, standing trustees and employees should use only trustee-owned laptops and storage media; hard drives on all laptops must be encrypted; and mobile storage media or the files on such media must be encrypted. Further, the USTP encourages standing trustees to retain a computer security consultant to review the proposed remote access solution and verify it meets industry security standards.

Another area of growing concern is employee misuse of computer resources. As set forth in the Handbook, standing trustees must now have an office policy that governs employees' use of the trustee's computer system, communicating to employees their responsibilities as users and the penalties for noncompliance. The policy should address employees' Internet access, personal use of the computer, personal email and personal instant messaging. All employees must sign the policy statement to acknowledge receipt and an understanding of their responsibilities. A sample policy statement is provided in supplemental materials accompanying the Handbook.

Conclusion

The updated Handbook clarifies the USTP's position on the duties owed by a standing trustee to debtors, creditors, other parties in interest and the U.S. Trustee. While this article highlights four important issues, we encourage trustees and trustee employees to continue to review the entire Handbook on the USTP’s Web site at their convenience.